

## Re: hacktool.rootkit

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-10/0276.html>

---

**From:** Shawn E. Hale (*SEHale\_at\_NOSPAMcomcast.net*)

**Date:** 10/21/05

Date: Fri, 21 Oct 2005 10:12:47 -0400

Thanks to you guys who replied with a wealth of advice and information. I appreciate that and the patience you have taken.

There is a lot to work through but so far, in addition to what I already listed, I did the things that were suggested in the Symantec site (re: safe mode virus scanning, registry entry purging, etc.). I also ran the Panda and Micro Trend online scans, safe mode virus scanning, system restore purging and turning back on, deleting temp files, and checking the downloaded applications folder. I also checked the running services and if I could not identify something, I googled it to see what it was. Everything was clean with no infected files and no bad services. I am leaning towards believing that I had initially wiped it out and the latest Symantec definitions caught an orphan. I was able to find a list of what was in the Symantec definitions that were downloaded on 10/19 and there was a piece that looked for the SVKP.sys file. Since I am not having any other slow downs and issues, I think I have it beat. I will get to Mr. Lipman's advice this weekend.

Thanks again.

"David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message news:uDFBPBc1FHA.2792@tk2msftngp13.phx.gbl...

> From: "Shawn E. Hale" <SEHale@NOSPAMcomcast.net>

>

> / I am trying to be as detailed about this as I can. Sorry if it is too long

> / but I figure more info is better than less. Using a new Dell laptop with XP

> / Home, SP2 and all updates. Norton Antivirus 2005 installed and set for

> / automatic updates. It is also set for real time (constant) scanning.

> /

> / 2 weeks ago (10/3/05) my daughter was using AOL IM when someone

> / inadvertently sent her a link which she followed and ran. Immediately all

> / of her other buddies on IM got the same link from her even though she didn't

> / manually forward it. Sensing something was wrong, she disconnected from the

microsoft.public.security.virus: Re: hacktool.rootkit

> / *IM. Norton Antivirus reported the following:*  
> /  
> / *Auto-Protect, Hacktool.rootkit, Access Denied. Source:*  
> / *c:\windows\system32\msdirectx.sys*  
> / *Auto-Protect, Hacktool.rootkit, Repair*